2 Забезпечення комп'ютерної безпеки в інформаційних системах

УДК 621.391.7

МЕТОДИ АВТЕНТИФІКАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницький національний технічний університет

Анотація: **Запропоновано методи автентифікації, що базуються на математичному апараті рекурентних V_k –послідовностей. Проведено дослідження криптографічної стійкості та обчислювальної складності, в результаті якого встановлено, що запропоновані методи є більш стійкими і за певних умов мають не меншу складність обчислень, ніж відомі аналоги. Показано також можливість перетворення запропонованих схем автентифікації в схеми цифрового підписування.**

Summary: **We propose authentication methods, based on mathematical apparatus of recurrent V_k sequences. We conducted a research on cryptographic reliability and computational complexity, whose results revealed that the proposed methods are more reliable, and under certain conditions have no less computational complexity than the known equivalents. We also show a possibility of converting the proposed authentication schemes into digital signature schemes.**

Ключові слова: **Захист інформації, криптографія, автентифікація, цифрове підписування, рекурентні послідовності.**

I Вступ

Забезпечення цілісності на сьогодні є не менш актуальною задачею, ніж забезпечення конфіденційності інформації. Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації використовують криптографічні протоколи [1–7]. Найбільш розповсюдженими є два типи криптографічних протоколів – автентифікації та цифрового підписування [1–7].

В загальному вигляді в схемі автентифікації сторін взаємодії [5] існує два учасника – претендент – сторона, яка повинна довести свою автентичність, та перевіряльник – сторона, яка цю автентичність повинна перевірити. Претендент має два ключа – загальнодоступний K_1 та секретний K_2. При доведенні автентичності з нульовим розголошенням претенденту необхідно довести, що він знає K_2, причому зробити це таким чином, щоб це доведення можна було б перевірити знаючи лише K_1.

Теоретичні основи схем автентифікації були закладені в роботі Сіммонса [8]. Найбільш відомими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1–4]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. Крім того актуальним залишається підвищення стійкості схем автентифікації.

В цьому зв'язку певний інтерес викликає апарат на основі рекурентних послідовностей [9, 10], який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач. Так в роботі [11] представлено метод автентифікації сторін взаємодії, який базується на рекурентних V_k^+ та U_k –послідовностях і який, порівняно з відомими методами, дозволяє суттєво спростити обчислення. Однак представлений метод не задовольняє усім вимогам до протоколів автентифікації, оскільки не дозволяє використовувати претенденту сеансовий ключ, хоча і в такому представленні має широке застосування. Виходячи з цього, актуальними є дослідження цих рекурентних послідовностей щодо розробки методу автентифікації, який би задовольняв усім вимогам.

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [12]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k}, \qquad (1)$$

де a_1, a_2, . . . , a_k – коефіцієнти, k – порядок послідовності, виходячи з початкових елементів u_0, u_1, …, u_k.

Певну цікавість представляють послідовності, в яких початкові елементи пов'язані з коефіцієнтами. Найпростішим прикладом в цьому випадку є послідовність, елементи якої обчислюються за формулою

$$u_n = a_1 \cdot u_{n-1}. \tag{2}$$

Якщо $u_1 = q$, $a_1 = q$, то $u_n = q^n$. Тобто, в цьому випадку, рекурентне співвідношення породжує степеневу послідовність.

Наступним за складністю є випадок, коли два коефіцієнти відрізняються від нуля. В цьому випадку елементи послідовності обчислюються за такою формулою

$$u_n = a_1 \cdot u_{n-1} + a_k \cdot u_{n-k}. \tag{3}$$

В [10] розглянуто V_k –послідовність, яка складається з V_k^+ –послідовності та V_k^- –послідовності.

V_k^+ –послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \tag{4}$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \tag{5}$$

V_k^- –послідовністю називається послідовність чисел, що обчислюються за формулою (5) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [9]

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \tag{6}$$

В окремому випадку, коли $m = n$ залежність (6) буде мати такий вигляд

$$v_{2n,k} = v_{n+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{n+(k-2)-i,k} \cdot v_{n-k+i,k}. \tag{7}$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [10]

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \tag{8}$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють розробити методи автентифікації на їх основі.

II Методи автентифікації на основі рекурентних V_k –послідовностей

Суть методу автентифікації, що пропонується (заявка на корисну модель № u 2013 06319 від 22.05.2013 р.), базується на використанні властивості (6) V_k –послідовності, яка дозволяє використовувати її для обчислення елементу $v_{n+m,k}$, а також для обчислення елементу $v_{-n+m,k}$. Крім того, властивість (6) дозволяє реалізувати процедуру обчислення елементу $v_{n \cdot m,k}$. Так само на основі властивості (8) можна

реалізувати процедуру обчислення елементу $v_{-n\cdot m,k}$. Все це дає можливість створення такого методу автентифікації.

Спочатку претендент (або центр довіри) виконує попередню процедуру обчислення ключів. Для цього він випадковим чином вибирає секретний ключ a, після чого обчислює і передає перевіряльнику відкритий ключ $v_{-a+i,k}$, $i=\overline{-k,-1}$.

Коли претендент хоче довести свою автентичність, він вибирає випадкове число b, обчислює $v_{b+i,k}$, $i=\overline{-k,k-2}$, визначає з цього набору елементів значення x як $x=v_{b,k}$ і передає його перевіряльнику. В цей час перевіряльник вибирає випадкове число c, обчислює $v_{c+i,k}$, $i=\overline{-(k-1),0}$, і передає ці елементи претенденту.

Потім претендент обчислює $v_{c\cdot a+i,k}$, $i=\overline{-1,k-2}$, на основі елементів $v_{c+i,k}$, $i=\overline{-(k-1),k-2}$, та секретного ключа a. В цей час перевіряльник обчислює $v_{-a\cdot c+i,k}$, $i=\overline{-(k-1),0}$, на основі елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, та свого сеансового ключа c.

Після цього претендент обчислює $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, використовуючи залежність (6), і передає ці елементи перевіряльнику. На завершення, перевіряльник використовує отримані елементи для обчислення x' як $x'=v_{-a\cdot c+(b+c\cdot a),k}$, використовуючи залежність (6), і перевіряє отримане значення зі значенням x, яке він раніше отримав від претендента.

Виходячи з цього схема автентифікації за даним методом буде мати такий вигляд (рис. 1).

Операція за модулем в схемі автентифікації використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Обчислення елементів $v_{b+i,k} \bmod p$, $i=\overline{-k,k-2}$, претендентом можуть бути виконані попередньо, заздалегідь до безпосередньої автентифікації.

В запропонованому методі автентифікації основні обчислення виконуються згідно з залежністю (6). Обчислення елементу $v_{n+m,k}$ згідно з цією залежністю здійснюється на основі елементів $v_{n+i,k}$, $i=\overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i=\overline{-1,k-2}$.

В разі необхідності отримання певного послідовного набору елементів V_k –послідовності у кількості, більшої ніж k, достатньо отримати будь-які послідовні k з них, оскільки інші можуть бути обчислені згідно з формулами (4) або (5) на основі вже отриманих.

Також слід зазначити, що для обчислення претендентом набору з k елементів $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, він може k разів використовувати залежність (6) для обчислення елементів цього набору як $v_{(b+i)+(c\cdot a),k}$, $i=\overline{-1,k-2}$. Тоді для кожного $v_{b+i,k}$, $i=\overline{-1,k-2}$, необхідно мати набір з $v_{(b+i)+j,k}$, $j=\overline{-(k-1),0}$, елементів. Виходячи з цього, всього для обчислення елементів $v_{b+c\cdot a+i,k}$, $i=\overline{-1,k-2}$, необхідно мати елементи $v_{b+i,k}$, $i=\overline{-k,k-2}$. Щоб отримати цей набір претенденту спочатку треба отримати $v_{b+i,k}$ для $i=\overline{-(k-1),k-2}$, а потім окремо для $i=-k$, використовуючи формулу (5).

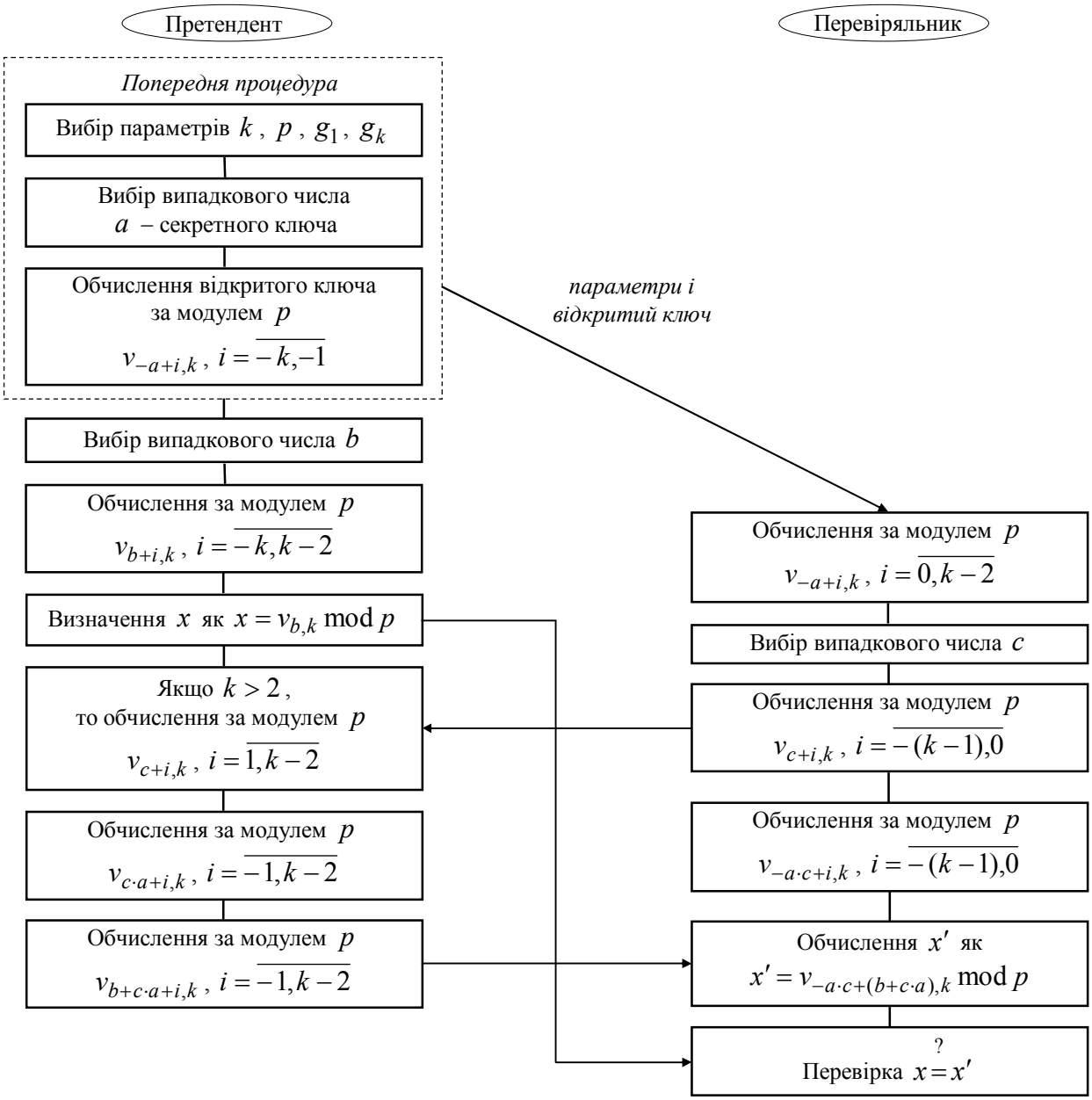

Рисунок 1 – Схема автентифікації на основі елементів V_k –послідовності

Визначивши як можуть отримуватись елементи V_k –послідовності, що використовуються в методі автентифікації, отримаємо такий протокол автентифікації.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати g_1, g_k.

П.4. Претенденту передати параметри Перевіряльнику.

П.5. Претенденту вибрати випадкове число a – секретний ключ.

П.6. Претенденту обчислити відкритий ключ за модулем p $v_{-a+i,k}$, $i=\overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П.7. Претенденту передати відкритий ключ $v_{-a+i,k} \bmod p$, $i = \overline{-k,-1}$, Перевіряльнику.

П.8. Перевіряльнику обчислити за модулем p $v_{-a+i,k}$, $i = \overline{0,k-2}$, за формулою (4).

П.9. Претенденту вибрати випадкове число b, а Перевіряльнику вибрати випадкове число c.

П.10. Претенденту обчислити за модулем p $v_{b+i,k}$, $i = \overline{-(k-1),k-2}$, а Перевіряльнику обчислити за модулем p $v_{c+i,k}$, $i = \overline{-(k-1),0}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.11. Претенденту обчислити за модулем p $v_{b-k,k}$ за формулою (5).

П.12. Претенденту визначити x як $x = v_{b,k} \bmod p$ і передати отримане значення Перевіряльнику.

П.13. Перевіряльнику передати $v_{c+i,k} \bmod p$, $i = \overline{-(k-1),0}$, Претенденту.

П.14. Претенденту перевірити, якщо $k > 2$, то обчислити за модулем p $v_{c+i,k}$, $i = \overline{1,k-2}$, використовуючи формулу (4).

П.15. Претенденту обчислити за модулем p $v_{c\cdot a+i,k}$, $i = \overline{-1,k-2}$, а Перевіряльнику обчислити за модулем p $v_{-a\cdot c+i,k}$, $i = \overline{-(k-1),0}$, використовуючи алгоритми прискореного обчислення елементів $v_{m\cdot n,k}$ та $v_{-m\cdot n,k}$, відповідно.

П.16. Претенденту обчислити за модулем p $v_{b+c\cdot a+i,k}$, $i = \overline{-1,k-2}$, за формулою (6) і передати отримані елементи Перевіряльнику.

П.17. Перевіряльнику обчислити $x' = v_{-a\cdot c+(b+c\cdot a),k} \bmod p$ за формулою (6) та порівняти отримане значення з x, тобто перевірити $x \overset{?}{=} x'$.

У п. 2 проводиться вибір параметру p, який є модулем при обчисленнях в представленому протоколі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

У п. 3 відбувається вибір параметрів g_1, g_k. Оскільки значення будь-якого числа в розробленому протоколі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

У п. 10 протоколу автентифікації необхідно здійснювати обчислення за модулем p елементів $v_{b+i,k}$, $i = \overline{-(k-1),k-2}$, а також елементів $v_{c+i,k}$, $i = \overline{-(k-1),0}$. Ці обчислення можна здійснювати за одним з алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які представлено в роботі [10].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i = \overline{-k,k-2}$, що виконуються у п. 6 протоколу автентифікації, на основі одного з запропонованих у тій же роботі [10] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п. 15 протоколу автентифікації необхідно здійснювати обчислення за модулем p елементів $v_{c\cdot a+i,k}$, $i = \overline{-1,k-2}$, на основі елементів $v_{c+i,k}$, $i = \overline{-k+1,k-2}$, та секретного ключа a, а також обчислення за модулем p елементів $v_{-a\cdot c+i,k}$, $i = \overline{-k+1,0}$, на основі $v_{-a+i,k}$, $i = \overline{-k,k-2}$, та сеансового ключа c Перевіряльника.

Тобто необхідно визначити процедуру обчислення елементів $v_{m\cdot n,k}$ та $v_{-m\cdot n,k}$ для V_k −послідовності.

Обчислення елементу $v_{m\cdot n,k}$ може здійснюватись за формулою (4) на основі елементу $v_{m,k}$. Однак, безпосереднє обчислення $v_{m\cdot n,k}$ за цією формулою є повільним, а тому не може бути використано для великих значень n. Виникає необхідність у більш швидкому методі обчислення елементу $v_{m\cdot n,k}$.

В цьому зв'язку слід звернути увагу на запропонований в [10] метод прискореного обчислення елементу $v_{n,k}$. Метод базується на тій же ідеї, що і бінарний метод [13] піднесення до степеня, в якому отримується адитивний ланцюжок

$1 = c_0, c_1, c_2, \ldots, c_t = n$.

Якщо записати n в двійковій системі числення як $n = \sum_{i=0}^{t} \alpha_{t-i} 2^{t-i}$, то для кожного $i = \overline{1,t}$ правило отримання адитивного ланцюжка, починаючи з c_1, буде таким

– якщо значення α_{t-i} дорівнює 0, то $c_i = 2c_{i-1}$;

– якщо значення розряду α_{t-i} дорівнює 1, то $c_i = 2c_{i-1} + 1$.

Як наслідок, дійшовши до крайнього правого розряду *n*, отримаємо $c_t = n$.

Згідно з цим методом обчислення елементу $v_{n,k}$ зводиться до послідовного обчислення $v_{c_i,k} = v_{2c_{i-1}+1,k}$ або $v_{c_i,k} = v_{2c_{i-1},k}$. При цьому обчислення $v_{c_i,k} = v_{2c_{i-1},k}$ здійснюється згідно з залежністю (7), а $v_{c_i,k} = v_{2c_{i-1}+1,k}$ отримується, обчислюючи спочатку $v_{2c_{i-1},k}$, а потім $v_{2c_{i-1}+1,k}$ за формулою (4).

Запропонований метод дозволяє здійснювати прискорене обчислення елементу $v_{n,k}$, починаючи з елементів $v_{1+i,k}$, $i = \overline{-(k-1),k-1}$. При цьому не важко помітити, що якщо починати ці обчислення з елементів $v_{m+i,k}$, $i = \overline{-(k-1),k-1}$, то ми отримаємо метод прискореного обчислення елементу $v_{m\cdot n,k}$.

Використовуючи l як поточне значення індексу елементу V_k–послідовності, отримаємо такий алгоритм прискореного обчислення елементів $v_{m\cdot n,k}$ цієї послідовності.

Алгоритм 1.

П.1. Провести початкову ініціалізацію: $i \leftarrow t$; $l \leftarrow m$; присвоїти елементам $v_{l+k-1,k}, \ldots, v_{l-(k-2),k}$, $v_{l-(k-1),k}$ відповідні значення V_k–послідовності.

П.2. $i \leftarrow i - 1$.

П.3. $l \leftarrow 2l$.

П.4. Обчислити нові значення $v_{l+1,k}$, $v_{l,k}, \ldots, v_{l-(k-3),k}$, $v_{l-(k-2),k}$ за модулем p, використовуючи (6).

П.5. Обчислити елемент $v_{l-(k-1),k}$ за модулем p, використовуючи (5).

П.6. Якщо $k > 2$, то обчислити елементи $v_{l+k-1,k}$, $v_{l+k-2,k}, \ldots, v_{l+3,k}$, $v_{l+2,k}$ за модулем p, використовуючи (4).

П.7. Якщо $\alpha_i = 0$, то перейти до п. 10.

П.8. $l \leftarrow l + 1$.

П.9. Обчислити нові значення $v_{l+k-1,k}$, $\ldots$, $v_{l-(k-2),k}$, $v_{l-(k-1),k}$ шляхом присвоювання кожному попередньому елементу значення наступного за ним елементу та обчислення за модулем p останнього елементу $v_{l+k-1,k}$ за формулою (4), використовуючи тільки-но обчислені елементи.

П.10. Якщо $i - 1 \neq 0$, то перейти до п. 3, інакше завершити роботу алгоритму.

По аналогії з розглянутим методом прискореного обчислення елементу $v_{m\cdot n,k}$ можна отримати метод прискореного обчислення елементу $v_{-m\cdot n,k}$, використавши представлений в ті й же роботі [10] метод прискореного обчислення елементу $v_{n,k}$ для від'ємних n на основі бінарного методу. Тільки на відміну від цього методу для отримання методу прискореного обчислення елементу $v_{-m\cdot n,k}$ будемо здійснювати обчислення, починаючи з елементів $v_{-m+i,k}$, $i=\overline{-k,k-2}$, а не з $v_{-1+i,k}$ для тих же значень i.

Тоді отримаємо такий алгоритм прискореного обчислення елементів $v_{-m\cdot n,k}$ для V_k–послідовності.

Алгоритм 2.

П.1. Провести початкову ініціалізацію: $i \leftarrow t$; $l \leftarrow m$; присвоїти елементам $v_{-l+k-2,k}$, ..., $v_{-l-(k-1),k}$, $v_{-l-k,k}$ відповідні значення V_k–послідовності.

П.2. $i \leftarrow i-1$.

П.3. $l \leftarrow 2l$.

П.4. Обчислити нові значення елементів $v_{-l+k-2,k}$, ... , $v_{-l,k}$, $v_{-l-1,k}$, за модулем p, використовуючи (8).

П.5. Обчислити елементи $v_{-l-2,k}$, ... , $v_{-l-(k-1),k}$, $v_{-l-k,k}$, за модулем p, використовуючи (5).

П.6. Якщо $\alpha_i = 0$, то перейти до п. 9.

П.7. $l \leftarrow l+1$.

П.8. Обчислити нові значення $v_{-l+k-2,k}$, ... , $v_{-l-(k-1),k}$, $v_{-l-k,k}$ шляхом присвоювання кожному елементу значення попереднього елементу та обчислення за модулем p першого з цього набору елементу $v_{-l-k,k}$ за формулою (5), використовуючи тільки-но обчислені елементи.

П.9. Якщо $i-1 \neq 0$, то перейти до п. 3, інакше завершити роботу алгоритму.

Не важко помітити, що у випадку, якби $k=1$, запропонований метод автентифікації на основі рекурентних послідовностей практично перетворився б у метод Шнорра, принаймні став би йому дуже подібним.

Згідно з відомим протоколом автентифікації Шнорра [2] центр довіри або претендент вибирає і відкрито публікує два простих числа p і q, при цьому щоб q був співмножником $p-1$, та число $g \neq 1$ таке, що $g^q \equiv 1(\mathrm{mod}\, p)$. Потім він вибирає випадкове число $a < q$ як секретний ключ та обчислює $d = g^{-a} \bmod p$ – відкритий ключ, який передається перевіряльнику. Після цього протокол автентифікації реалізується таким чином.

1. Претендент вибирає випадкове число $b < q$, обчислює $x = g^b \bmod p$ і надсилає x перевіряльнику (ці обчислення можуть бути виконані і попередньо).

2. Перевіряльник виробляє випадкове число c: $0 < c \le 2^t - 1$ і надсилає його претенденту.

3. Претендент обчислює $y = b + a \cdot c(\mathrm{mod}\, q)$ і надсилає його перевіряльнику.

4. Перевіряльник перевіряє рівняння $x \overset{?}{=} g^y d^c \bmod p$.

Проведемо аналіз запропонованого методу автентифікації на основі елементів V_k–послідовності та порівняємо його з відомим методом автентифікації Шнорра.

Спочатку проведемо аналіз щодо криптографічної стійкості.

Здійснювати криптоаналіз запропонованого методу автентифікації на основі V_k–послідовності зловмисник може на основі відомих параметрів k, p, g_1, g_k, відкритого ключа $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, а також $v_{b,k} \bmod p$ і $v_{b+c\cdot a+i,k} \bmod p$, $i=\overline{-1,k-2}$, які передаються від претендента до

перевіряльника. Крім того, відомі елементи $v_{c+i,k} \bmod p$, $i = \overline{-(k-1),0}$, які передаються від перевіряльника до претендента.

Так само у методі Шнорра зловмиснику відомі параметри p, q, g, відкритий ключ $g^{-a} \bmod p$, а також $g^b \bmod p$ та $b + a \cdot c (\bmod q)$, які передаються від претендента до перевіряльника, та число c, яке передається від перевіряльника до претендента.

В роботі [9] досліджувалась стійкість криптографічних перетворень, що базуються на використанні елементів V_k^+ та U_k – послідовностей, з яких видно, що складність отримання зловмисником індексу елемента рекурентної послідовності, обчисленого за модулем, є принаймні не меншою, ніж отримання числа степеня з результату модулярного піднесення до степеня. Тобто можна вважати, що ці обчислення знаходяться приблизно на одному ж рівні.

Виходячи з цього можна стверджувати, що метод автентифікації на основі V_k–послідовності криптографічно є більш стійким, ніж відомий метод Шнорра, оскільки в ньому замість передавання числа c від перевіряльника до претендента та числа $b + a \cdot c (\bmod q)$ від претендента до перевіряльника відповідно передаються елементи $v_{c+i,k} \bmod p$, $i = \overline{-(k-1),0}$, та $v_{b+c\cdot a+i,k} \bmod p$, $i = \overline{-1,k-2}$, тобто не самі числа-індекси, а елементи рекурентної послідовності, обчислені для заданих індексів.

Перевагою запропонованого методу автентифікації на основі рекурентних послідовностей перед відомими методами щодо стійкості є також можливість змінювати параметр k, що, в свою чергу, дає можливість підвищувати криптостійкість за рахунок збільшення складності виконання протоколу автентифікації.

Також перевагою запропонованого методу автентифікації є те, що він має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Проведемо більш детальний аналіз запропонованого методу автентифікації щодо обчислювальної складності.

З результатів дослідження складності обчислення елементів V_k–послідовності, які наведено в роботі [10], видно, що складність обчислення елементу V_k–послідовності за алгоритмом його прискореного обчислення є значно більшою, ніж за будь-якою аналітичною залежністю обчислення елементів цієї послідовності.

Так само у відомому методі автентифікації Шнорра обчислювальна складність операції піднесення до степеня є значно більшою, ніж будь-якої іншої операції, що використовується в даному методі.

Аналіз запропонованого та відомого методів автентифікації показує, що згідно з запропонованим методом необхідно п’ять разів проводити обчислення елементів V_k–послідовності за прискореним алгоритмом, а саме обчислення за модулем p різних наборів елементів з $v_{-a,k}$, $v_{b,k}$, $v_{c,k}$, $v_{c\cdot a,k}$ та $v_{-a\cdot c,k}$. В той час як за відомим методом Шнорра необхідно виконувати чотири таких піднесення до степеня за модулем p: g^{-a}, g^b, g^y, та $(g^{-a})^c$.

В роботі [10] проведено дослідження складності виконання алгоритмів прискореного обчислення елементів V_k–послідовності, з якого видно, що складність обчислення елементу цієї послідовності із заданим індексом має приблизно такий же рівень, як і піднесення до заданого степеня того ж порядку, що й індекс.

Виходячи з цього, обчислювальна складність запропонованого методу автентифікації на основі V_k–послідовності є дещо більшою, ніж відомого методу Шнорра. Крім того, перевагою останнього є також те, що в ньому сторони автентифікації передають по одному числу, в той час як згідно з запропонованим методом сторони автентифікації, крім випадку передавання $x = v_{b,k} \bmod p$, передають набори з k елементів V_k–послідовності.

Однак, вказана перевага досягається завдяки меншій стійкості відомого методу, ніж запропонованого. В такому випадку слід враховувати, що запропонований метод можна спростити за рахунок зменшення стійкості до рівня, що наближується до рівня відомого методу, якщо перевіряльнику не обчислювати і не

передавати елементи $v_{c+i,k} \bmod p$, $i = \overline{-(k-1),0}$, а одразу передавати лише сам індекс c (заявка на корисну модель № u 2013 06320 від 22. 05. 2013 р.). Тоді претендент буде обчислювати елементи $v_{(b+c\cdot a)+i,k} \bmod p$, $i = \overline{-1,k-2}$, одразу на основі індексу $b + c \cdot a$, оскільки йому вже стануть відомі всі числа, що цей індекс визначають. В результаті кількість чисел, що передаються між сторонами автентифікації, стане меншою і обчислювальна складність методу зменшиться до чотирьох обчислень елементів V_k –послідовності за прискореним алгоритмом, а саме до обчислень за модулем p з боку претендента відкритого ключа $v_{-a+i,k} \bmod p$, $i = \overline{-k,-1}$, елементу $v_{b,k} \bmod p$ та елементів $v_{b+c\cdot a+i,k} \bmod p$, $i = \overline{-1,k-2}$, а також з боку перевіряльника – елементів $v_{-a\cdot c+i,k}$, $i = \overline{-(k-1),0}$, тобто три обчислення з боку претендента, та одне – з боку перевіряльника. Необхідність виконання в такому випадку перевіряльником лише одного обчислення елементів V_k –послідовності замість двох піднесень до степеня згідно з відомим методом дає важливу перевагу перед відомим методом, оскільки існує багато задач, де процедуру перевірки автентичності необхідно здійснювати в реальному часі від великої кількості претендентів. В таких випадках перевіряльник за одиницю часу може отримувати велику кількість запитів на перевірку автентичності, що в свою чергу, може створювати для нього проблему перенавантаження. До такого роду задач відносяться задачі авторизації та ідентифікації під час здійснення трансакцій в електронних платіжних системах та в системах стільникового зв'язку, забезпечення веб-трансакцій між клієнтом та сервером, автентифікації в безпровідних мережах, організації банківських трансакцій, організації мобільної комерції, авторизації електронних повідомлень та інші.

Можна ще більше спростити запропонований метод автентифікації за рахунок зменшення криптостійкості, якщо перевіряльнику, окрім передавання лише самого індексу c, ще й не обчислювати $v_{(b+c\cdot a)+i,k} \bmod p$, $i = \overline{-1,k-2}$, а передавати лише саме число $b + c \cdot a$ і обчислення відповідних елементів V_k –послідовності для цього індексу за прискореним алгоритмом здійснювати вже перевіряльнику (заявка на корисну модель № u 2013 06321 від 22. 05. 2013 р.). В результаті кількість чисел, що передаються між сторонами автентифікації, стане ще меншою, ніж в попередньому варіанті запропонованого методу, при цьому загальна обчислювальна складність методу буде такою ж, як і в попередньому варіанті – чотири обчислення елементів V_k –послідовності за прискореним алгоритмом, але тепер претендент і перевіряльник будуть виконувати по два таких обчислення на кожному боці.

Є й інший шлях зменшення обчислювальної складності запропонованого методу автентифікації на основі V_k –послідовності за рахунок зменшення його криптографічної стійкості до рівня, наближеного до рівня відомого методу. Можна відповідно зменшувати розмір чисел та елементів послідовності, який в основному визначається параметром p методу. Тоді зменшиться і загальний розмір чисел, що передаються між сторонами автентифікації, і, як наслідок, зменшиться і обчислювальна складність запропонованого методу.

Відомо [3, 4], що будь-який метод автентифікації, що базується на технології відкритого ключа, може бути перетворений у метод цифрового підписування шляхом заміни перевіряльника однонаправленою хеш-функцією. При цьому повідомлення не хешується перед підписанням, замість цього хеш-функція включається в сам алгоритм цифрового підписування.

Виходячи з цього, запропонований метод автентифікації на основі V_k –послідовності може бути перетворений в такий метод цифрового підписування (заявка на корисну модель № u 2013 06322 від 22. 05. 2013 р.).

Спочатку відправник-підписант (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. При цьому він випадковим чином вибирає секретний ключ a, за допомогою якого обчислює, а потім передає одержувачу-перевіряльнику відкритий ключ $v_{-a+i,k}$, $i = \overline{-k,-1}$.

При формуванні цифрового підпису для повідомлення M відправник-підписант вибирає випадкове число b, обчислює $v_{b,k}$, визначає значення x як $x = v_{b,k}$ та обчислює хеш-значення r як $r = h(x, M)$ за допомогою обраної функції хешування h від повідомлення M та значення x. Далі він визначає

значення s як $s = b + a \cdot r$ і обчислює для нього елементи $v_{s+i,k}$, $i = \overline{-1, k-2}$. Після цього отриману множину цілих чисел $\{r; v_{s+i,k}, i = \overline{-1, k-2}\}$ він перетворює у цифровий підпис вигляду $DS = (0 \| r \| 0 \| v_{s-1,k} \| 0 \| v_{s,k} \| ... 0 \| v_{s+(k-2),k})$ і передає його разом з повідомленням M одержувачу.

При перевірці цифрового підпису одержувач спочатку обчислює $v_{-a \cdot r+i,k}$, $i = \overline{-(k-1), 0}$, на основі відкритого ключа – елементів $v_{-a+i,k}$, $i = \overline{-k, k-2}$, та отриманого від підписанта значення r. Потім він обчислює x' як $x' = v_{-a \cdot r+s,k}$, використовуючи залежність (6), обчислює хеш-значення r' як $r' = h(x', M)$ та перевіряє, чи виконується $r \overset{?}{=} r'$. Якщо так, то підпис приймається, в іншому випадку – відкидається.

Для обмеження розрядності чисел всі операції в методі слід виконувати за модулем.

Цікаво, що даний метод цифрового підписування дозволяє одразу вирішити дві проблеми – підвищити стійкість цифрового підписування, оскільки замість числа s згідно з відомим методом тепер передається елемент послідовності $v_{s,k}$ з відповідним індексом, а також суттєво спростити обчислювальну складність процедури перевірки підпису, оскільки замість двох піднесень до степеня згідно з відомим методом тепер необхідно виконувати лише одне обчислення елементу $v_{-a \cdot r,k}$ за прискореним алгоритмом обчислення елементів V_k–послідовності. І хоча при цьому виникає необхідність при формуванні підпису виконувати три обчислення елементів V_k–послідовності за прискореним алгоритмом замість двох піднесень до степеня згідно з відомим методом, однак існує багато задач, в яких перевірку цифрового підпису необхідно здійснювати значно частіше, ніж його формування, або перевіряти підпис від великої кількості його власників, як то в клієнт-серверних задачах. Тому при вирішенні такого роду задач запропонований метод цифрового підписування володіє важливою перевагою перед відомими аналогами.

Слід також враховувати, що в даному методі цифрового підписування теж можна спростити обчислення, змінивши їх шляхом уникнення необхідності обчислення набору елементів для $v_{s,k}$, який передається потім від підписанта одержувачу, і передавати лише саме значення s по аналогії з відомим методом (заявка на корисну модель № u 2013 06323 від 22. 05. 2013 р.).

III Висновки

На основі математичного апарату рекурентних V_k–послідовностей запропоновано метод автентифікації, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. Представлено протокол реалізації методу а також необхідні для цієї реалізації алгоритми прискореного обчислення елементів V_k–послідовності з можливістю мультиплікативної зміни індексу послідовності.

Проведено дослідження та здійснено порівняльний аналіз запропонованого методу автентифікації з відомим методом Шнорра щодо криптографічної стійкості та обчислювальної складності. Встановлено, що запропонований метод є більш стійким, ніж відомий аналог, при цьому він ще й дозволяє змінювати стійкість методу залежно від параметру k–порядку послідовності. Крім того метод, що запропоновано, має значно простішу процедуру завдання параметрів.

Оскільки відомий метод має меншу обчислювальну складність і потребує меншої кількості чисел, що передаються між сторонами автентифікації, то запропоновано декілька варіантів методу автентифікації на основі V_k–послідовностей, які дозволяють за рахунок зменшення стійкості до рівня відомого методу зменшити обчислювальну складність та кількість чисел, що передаються між сторонами автентифікації. Зокрема, один з таких варіантів методу порівняно з відомим аналогом дозволяє зменшити обчислювальну складність з боку перевіряльника.

Показано можливість перетворення запропонованої схеми автентифікації в схему цифрового підписування. Представлено дві схеми цифрового підписування на основі V_k–послідовностей, які

забезпечують порівняно з відомими аналогами підвищення стійкості цифрового підписування, а також спрощення процедури перевірки підпису, що особливо важливо для клієнт-серверних задач.

Література: ***1.*** *Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p.* ***2.*** *Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. – М.: Горячая линия–Телеком, 2007. – 320 с.* ***3.*** *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.* ***4.*** *Романец Ю. В., Тимофеева П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.* ***5.*** *Введение в криптографию / Под общ. ред. В. Б. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 236 с.* ***6.*** *Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.* ***7.*** *Брассар Ж. Современная криптология. – М.: ПОЛИМЕД, 1999. – 176 с.* ***8.*** *Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411–431.* ***9.*** *Яремчук Ю. Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем // Захист інформації. – № 4, 2012. – С. 120–127.* ***10.*** *Яремчук Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань // Реєстрація, зберігання і обробка даних. – Т. 15, № 1, 2013. – С. 14–22.* ***11.*** *Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей // Сучасний захист інформації. – № 1, 2013. – С. 4–10.* ***12.*** *Маркушевич А. И. Возвратные последовательности. – М.: Наука, 1975. – 48 с.* ***13.*** *Кнут Д. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. – М.: Вильямс, 2004. – 832 с.*

УДК: 004.056.5

ОЦІНЮВАННЯ СТІЙКОСТІ МЕТОДУ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ ДО АКТИВНИХ ТА ПАСИВНИХ АТАК

Василь Карпінець, Юрій Яремчук, Кирило Безпалий
Вінницький національний технічний університет

Анотація: **Проведено аналіз стійкості методу вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення до активних та пасивних зловмисних атак, спрямованих на зчитування та ускладнення витягнення ЦВЗ правовласником. Для цього були розглянуті поширені атаки на основі афінних перетворень зображення, атака шляхом внесення додаткового шуму, а також пасивна атака для визначення місця розташування ЦВЗ. Результати аналізу показали високий рівень стійкості методу до цих атак завдяки особливостям вбудовування ЦВЗ і використаного двовимірного дискретного косинусного перетворення.**

Summary: **This paper analyzes the stability of the method of embedding digital watermarks (digital watermark) in vector images for active and passive malicious attacks aimed at reading and complications extract digital watermark owner. This was considered common attacks based on affine transformations of the image, the attack by introducing additional noise, and passive attack is to determine the location of digital watermark. The analysis showed a high level of resistance to this attack method by digital watermark embedding features and used two-dimensional discrete cosine transform.**

Ключові слова: **Стеганографія, цифровий водяний знак, захист авторського права, векторні зображення, стеганографічна стійкість.**

І Вступ

Задача захисту авторського права векторних зображень на сьогодні стає все більш актуальною. Особливу увагу привертають такі методи забезпечення захисту, для яких не потрібно наявності оригіналу для підтвердження авторства. На сьогодні запропоновано декілька таких методів вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення [1]. Проте недоліком таких методів є можливі значні спотворення зображення внаслідок вбудовування ЦВЗ. У роботі [2] запропоновано метод, який забезпечує збереження високого рівня якості зображення при вбудовуванні ЦВЗ [3].

Однак, актуальним залишається питання аналізу запропонованого методу щодо забезпечення стійкості до зловмисних атак. У роботах [4] та [5] було проведено дослідження стеганографічної стійкості методу до відомих активних і пасивних атак, спрямованих на зчитування, видалення або підміну ЦВЗ, а також на ускладнення витягування правовласником ЦВЗ шляхом додавання шуму, видалення/додавання точок